UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/741,798	12/19/2003	Susan Pittman Dark	58895/P001C1/10316486	5599

29053   7590   10/03/2008
FULBRIGHT & JAWORSKI L.L.P
2200 ROSS AVENUE
SUITE 2800
DALLAS, TX 75201-2784

EXAMINER
RUTKOWSKI, JEFFREY M

ART UNIT	PAPER NUMBER
2619	

MAIL DATE	DELIVERY MODE
10/03/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 December 2003*.
2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-74* is/are pending in the application.
   4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) *1-74* is/are rejected.
7)☐ Claim(s) _____ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☒ The drawing(s) filed on *19 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.
   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a)☐ All   b)☐ Some * c)☐ None of:
      1.☐ Certified copies of the priority documents have been received.
      2.☐ Certified copies of the priority documents have been received in Application No. _____.
      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
   Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Information Disclosure Statement

1.　　　The Examiner has taken note of the Applicant's supplemental communication, filed on

09/07/2006, where an English translation was supplied for the CA and CB references.

Claim Rejections - 35 USC § 112

2.　　　The following is a quotation of the first and second paragraphs of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.
> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3.　　　**Claims 1-11 and 33-47** are rejected under 35 U.S.C. 112, first paragraph, as failing to

comply with the enablement requirement. The claim(s) contains subject matter which was not

described in the specification in such a way as to enable one skilled in the art to which it pertains,

or with which it is most nearly connected, to make and/or use the invention. The specification

does not adequately describe how the information of a receiving device is gathered.

4.　　　**Claims 17-22 and 26-27** are rejected under 35 U.S.C. 112, first paragraph, as being a

single means (system for tracking data flow) claim.

5.　　　**Claims 1-16** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for

failing to particularly point out and distinctly claim the subject matter which applicant regards as

the invention.

6.　　　**Claims 1-16, 31-32, 51-53** are indefinite because it is not clear what is meant by a

feedback network because usually there is a device in the network that is performing the action

and the network is just used as a transport medium.

7.   **Claim 3** is indefinite because it is not clear what is meant by "pre-established criteria". It

is also not clear what the limits are being set on and which device is comparing and storing

information.

8.   **Claims 12-14** are indefinite because it is unclear what is meant by "...said last-mentioned

gathered data..."

9.   **Claims 31-32 and 51-53** are indefinite because the wherein clause in **claims 31 and 51**

are confusing.

Claim Rejections - 35 USC § 103

10.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

11.   The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459

(1966), that are applied for establishing a background for determining obviousness under 35

U.S.C. 103(a) are summarized as follows:

1.   Determining the scope and contents of the prior art.
2.   Ascertaining the differences between the prior art and the claims at issue.
3.   Resolving the level of ordinary skill in the pertinent art.
4.   Considering objective evidence present in the application indicating obviousness
        or nonobviousness.

12.   **Claims 1-3, 8-9, 11, 15-18, 22, 26-28, 31-35, 40-41, 44-45, 47-48, 51-55, 59, 63-67 and**

74 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf et al. (US Pat

6,415,321), hereinafter referred to as Gleichauf in view of Eschelbeck et al. (US Pat 6,611,869),

hereinafter referred to as Eschelbeck and Smith et al. ("Operating Firewalls Outside the LAN

Perimeter").

13.   For **claims 1, 33 and 65**, Gleichauf discloses a network environment where packets that

are received over the Internet (temporally available network) is received at a router **14** (gateway

router) that serves the purpose of directing packets via firewall **16** to either a web server **30** or a

file server **34** (receiving devices) based upon address information **[col. 4 line 67 to col. 5 line**

15]. Gleichauf's network environment further includes an Intrusion Detection System (IDS) **18**

and a domain mapping system **46 [figure 3]**. The domain mapping system **46**, which is part of a

monitoring system, has an acquisition engine **48** that is used to gather operational information

which, inter alia, includes such as Operating System (OS) type, services offered and potential

vulnerabilities, on network devices (receiving devices). The information is gathered by the

acquisition engine **48** via actively querying the network devices, polling or having the network

devices push information **[col. 5 line 45 to col. 6 line 30]**.

14.   Gleichauf discloses the IDS **18** uses the information stored in the domain mapping

system **46** to provide protection for the network devices, such as file server **34 [col. 6 lines 48-**

65]. Gleichauf does not disclose what happens if the IDS **18** detects an attack. Eschelbeck

discloses when an attack is detected by an IDS, a message is sent to the firewall via network

(feedback network) to have the firewall update it's Access Control List (ACL) (modify

operational characteristics) to prevent traffic from the source of the attack from entering the

network **[col. 6 lines 4-25]**. It would have been obvious to a person of ordinary skill in the art at

the time of the invention to use Eschelbeck's IDS in Gleichauf's invention to provide an active

security management environment **[Eschelbeck, abstract]**.

15.   The combination of Gleichauf and Eschelbeck disclose the active security management

of a firewall. The combination of Gleichauf and Eschelbeck do not disclose the active security

management of a gateway router. Smith discloses traditionally routers performed firewall

functions via ACL [Section 1 2nd paragraph]. Smith also discloses the use of gateway-

firewalls to protect networks [Section 3, Section 3.4 last paragraph]. It would have been

obvious to a person of ordinary skill in the art at the time of the invention to perform active

security management on the ACL of a gateway router in Gleichauf's invention to block attacks

as close to the source of the attack as possible [Section 3, 2nd paragraph].

16.   Specifically for claim 65, Gleichauf discloses the IDS 48 can be placed in any location in

the network, including a firewall [col. 5 lines 10-13]. Which suggests an architecture where

packets are stored (database for future delivery) and then scanned before being transferred to the

destination device.

17.   For claims 2, 34 and 66, Gleichauf discloses that Simple Network Management Protocol

(SNMP) queries (certain data contained in one or more messages) can be used to gather

information [col. 6 lines 23-25].

18.   For claims 3, 18, 35, 55 and 67, Gleichau discloses the use of signature matching, where

packets are compared to "attack signatures" (pre-established criteria), and pattern matching are

known methods to detect attacks [col. 1 lines 25-30].

19.   Gleichau does not disclose setting limits. Smith suggests the setting of limits by

disclosing an firewall and IDS system that detects Denial-of-Service attacks [Section 1 page

494]. Since DoS attacks work by causing a victim device to overflow its buffers by sending a

large number of requests in a short amount of time, it would have been obvious to a person of

ordinary skill in the art at the time of the invention to set limits to stop a DoS attack before the victim device "crashes".

20.   Glecichau also does not disclose adjusting ACL rules when an DoS attack is detected. Smith discloses a system that detects DoS attacks and routers traditionally performed firewall functions via ACL **[Section 1 page 494, Section 1 2nd paragraph]**. It would have been obvious to a person of ordinary skill in the art at the time of the invention to perform active security management on the ACL of a gateway router based upon set limits in Gleichauf's invention to block attacks as close to the source of the attack as possible **[Section 3, 2nd paragraph]**.

21.   For **claim 8**, Gleichau's invention takes into account that information changes dynamically by actively collecting information from network devices **[col. 5 line 45 to col. 6 line 30]**.

22.   For **claims 9 and 41**, Gleichauf does not disclose the blocking of certain packets from reaching a destination. Eschelbeck discloses ACL is updated to prevent any more traffic from the source of the attack from entering the network **[col. 6 lines 4-25]**. It would have been obvious to a person of ordinary skill in the art at the time of the invention to use Eschelbeck's IDS in Gleichauf's invention to provide an active security management environment **[Eschelbeck, abstract]**.

23.   For **claims 11 and 74**, Gleichau suggests an IDS **18**, which is part of a monitoring system, that can be used to monitor traffic leaving a network device (receiving device) because the IDS **18** monitors network traffic as a whole **[col. 5 lines 5-8, figure 3]**.

24.   Gleichau does not disclose a gateway router where the ACL is modified according to outbound traffic. Smith contemplates the use of outbound traffic gateway firewalls **[Section 4]**. Given that Smith is concerned with stopping attacks as close to the source as possible and ACLs are used to keep one node from accessing another node **[Sections 1 and 3.4]**, it would have been obvious to a person of ordinary skill in the art at the time of the invention to block egress traffic via router gateway ACL to prevent an attack from the inside of the network.

25.   For **claims 15, 27, 31, 45, 51 and 64**, Gleichauf does not disclose changing ACL rules in a remote system. Smith discloses that in a corporate network, when a firewall detects an attack, messages are sent to remote gateway-firewalls (remote communication system) to have the attacker blocked (modify operational characteristics) **[Section 3.4]**. It would have been obvious to a person of ordinary skill in the art at the time of the invention to perform remote ACL management of a gateway router in Gleichauf's invention to block attacks as close to the source of the attack as possible **[Section 3, 2nd paragraph]**.

26.   For **claims 16 and 52-53**, Gleichauf discloses the use of an enterprise system **[figure 3]**.

27.   For **claims 17, 28, 48 and 54**, Gleichauf discloses an IDS **18** (system for tracking data flow; means for real time review) that is used to perform a pattern matching (identification of a specific data pattern; means for comparing) **[col. 1 lines 25-30, figure 3]**.

28.   Gleichauf discloses the IDS **18** uses the information stored in the domain mapping system **46** to provide protection for the network devices, such as file server **34 [col. 6 lines 48-65]**. Gleichauf does not disclose what happens if the IDS **18** detects an attack. Eschelbeck discloses when an attack is detected by an IDS, a message is sent to the firewall via network (send instructions from time to time; means for feeding) to have the firewall update it's ACL to

prevent traffic from the source of the attack from entering the network [col. 6 lines 4-25]. It would have been obvious to a person of ordinary skill in the art at the time of the invention to use Eschelbeck's IDS in Gleichauf's invention to provide an active security management environment [Eschelbeck, abstract].

29.   The combination of Gleichauf and Eschelbeck disclose the active security management of a firewall. The combination of Gleichauf and Eschelbeck do not disclose the active security management of a gateway router (control device). Smith discloses traditionally routers performed firewall functions via ACL [Section 1 2nd paragraph]. Smith also discloses the use of gateway-firewalls to protect networks [Section 3, Section 3.4 last paragraph]. It would have been obvious to a person of ordinary skill in the art at the time of the invention to perform active security management on the ACL of a gateway router in Gleichauf's invention to block attacks as close to the source of the attack as possible [Section 3, 2nd paragraph].

30.   For claims 22 and 59, Gleichauf discloses the use of an hypercube storage 50 (database).

31.   For claims 26, 32 and 63, figure 3 of Gleichauf shows the gateway router 14 of the local site (gateway unique to a particular location) is the gateway router whose ACL is modified

32.   For claim 40, Gleichau discloses a pattern analysis technique where packets are compared to "attack signatures" [col. 1 lines 25-30].

33.   For claim 44, figure 3 of Gleichauf shows the gateway router 14 of the local site (particular location) is the gateway router whose ACL is modified.

34.   For claim 47, Gleichauf discloses gathered network information is stored in a hypercube storage 50 [figure 3].

35.   **Claims 4-5, 19, 21, 29, 36-37, 49, 56, 58 and 68-69** are rejected under 35 U.S.C. 103(a)

as being unpatentable over Gleichauf in view of Eschelbeck and Smith as applied to **claims 3,**

18, 28,35 and 67 respectively above, and further in view of Kouznetsov (US Pat 6,725,377).

36.   For **claims 4, 19, 29, 36, 49, 56 and 68**, the combination of Gleichauf, Eschelbeck and

Smith does not disclose the dynamic adjustment of thresholds. Kouznetsov discloses an

mechanism where profiles, that contain attack signatures and thresholds **[col. 2 lines 53-60]**, are

updated automatically **[col. 8 lines 26-30]**. It would have been obvious to a person of ordinary

skill in the art at the time of the invention to use dynamic limits in Gleichauf's invention to take

into account newly detected attack patterns **[Kouznetsov, abstract]**.

37.   For **claims 5, 21, 37, 58 and 69**, the combination of Gleichauf, Eschelbeck and Smith

does not disclose the manual adjustment of thresholds. Kouznetsov discloses a user decides

which attack signatures are to be included in the profile, which results in a manual adjustment of

detection thresholds **[col. 2 lines 53-65]**. It would have been obvious to a person of ordinary

skill in the art at the time of the invention to use manually adjusted limits in Gleichauf's

invention to take into account new attack patterns **[Kouznetsov, abstract]**.

38.   **Claims 6-7, 10, 12-14, 20, 23-25, 38-39, 43, 46, 57, 60-62, 70-73** are rejected under 35

U.S.C. 103(a) as being unpatentable over Gleichauf in view of Eschelbeck and Smith as applied

to **claims 1, 17, 18, 29, 33 and 65 respectively** above, and further in view of Conklin et al. (US

Pat 5,991,881) hereinafter referred to as Conklin.

39.   For **claims 6, 38 and 70**, the combination of Gleichauf, Eschelbeck and Smith discloses

the gathering of information from a network device. The combination of Gleichauf, Eschelbeck

and Smith does not disclose the statistical comparison of gathered information. Conklin

discloses a attack detection process where captured packets (gathered information) is compared against historical information that was collected over time [**col. 7 lines 50-55**]. It would have been obvious to a person of ordinary skill in the art at the time of the invention to use Conklin's detection mechanism in Gleichauf's invention to use of artificial intelligence to detect attacks [**Conklin, col. 7 line 53**].

40.   For **claims 7, 20, 39 50, 57 and 71**, the combination of Gleichauf, Eschelbeck and Smith does not disclose the gathering of statistics to reflect normal behavior. Conklin disclosure that artificial intelligence techniques can be used to detect attacks, suggests gathering statistics to reflect normal behavior [**col. 7 lines 50-55**]. It would have been obvious to a person of ordinary skill in the art at the time of the invention to collect statistics to reflect normal behavior in Gleichauf's invention to "feed" the artifical intelligence engine.

41.   For **claims 10, 43 and 73**, the combination of Gleichauf, Eschelbeck and Smith does not disclose the storage of received packets. Conklin discloses an IDS process where incoming packets is stored [**figure 7**]. It would have been obvious to a person of ordinary skill in the art at the time of the invention to use Conklin's detection mechanism in Gleichauf's invention to use of artificial intelligence to detect attacks [**Conklin, col. 7 line 53**]. It would have been obvious to a person of ordinary skill in the art at the time of the invention to store packet information in Gleichauf's invention to allow for the use of artificial intelligence to detect attacks [**Conklin, col. 7 line 53**].

42.   For **claims 12, 23, 46 and 60**, the combination of Gleichauf, Eschelbeck and Smith does not disclose gathering packet information. Conklin discloses packets are collected and statistical information from the packets is stored (information about the history of the packets) [**figure 7**].

It would have been obvious to a person of ordinary skill in the art at the time of the invention to gather packet information in Gleichauf's invention to use artificial intelligence to detect an attack.

43.   For **claims 13, 24 and 61**, Gleichauf discloses the storing information to be used by an IDS **18** system **[col. 6 lines 50-55, figure 3]**.

44.   For **claims 14, 25 and 62**, Gleichauf discloses the IDS **18** obtains a vulnerabilities list (selected data) that is grouped by OS (parameters of receiving device) and incidence **[col. 6 lines 62-65]**.

45.   For **claim 72**, Gleichau discloses a pattern analysis technique where packets are compared to "attack signatures" **[col. 1 lines 25-30]**.

46.   **Claims 30 and 50** are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf in view of Eschelbeck, Smith and Kouznetsov as applied to **claims 29 and 49 respectively** above, and further in view of Conklin.

47.   For **claims 7, 20, 39 50**, the combination of Gleichauf, Eschelbeck, Smith and Kouznetsov does not disclose the gathering of statistics to reflect normal behavior. Conklin disclosure that artificial intelligence techniques can be used to detect attacks, suggests gathering statistics to reflect normal behavior **[col. 7 lines 50-55]**. It would have been obvious to a person of ordinary skill in the art at the time of the invention to collect statistics to reflect normal behavior in Gleichauf's invention to "feed" the artifical intelligence engine.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEFFREY M. RUTKOWSKI whose telephone number is (571)270-1215. The examiner can normally be reached on Monday - Friday 7:30-5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hassan Kizou can be reached on (571) 272-3088. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffrey M Rutkowski
Patent Examiner
09/29/2008

/Hassan Kizou/
Supervisory Patent Examiner, Art Unit 2619